Software Safety Requirements and Architecture

Lane Assistance

Document Version: 1.0

Template Version 2.0, Released on 2017-10-17

Document History

Date	Version	Editor	Description
2017-10-16	1.0	Daniel Gattringer	Initial version

Table of Contents

1. Purpose

The creation of Software Safety Requirements and the refining of the architecture are part of the safety process of ISO 26262 for the treatment of potential malfunctions in electrical and electronic systems.

The purpose of the Software Safety Requirements and the refining of the architecture is to identify new detailed software requirements and allocate them to component level diagrams of the lane assistance functional safety project.

2. Inputs to the Software Requirements and Architecture Document

2.1. Technical safety requirements

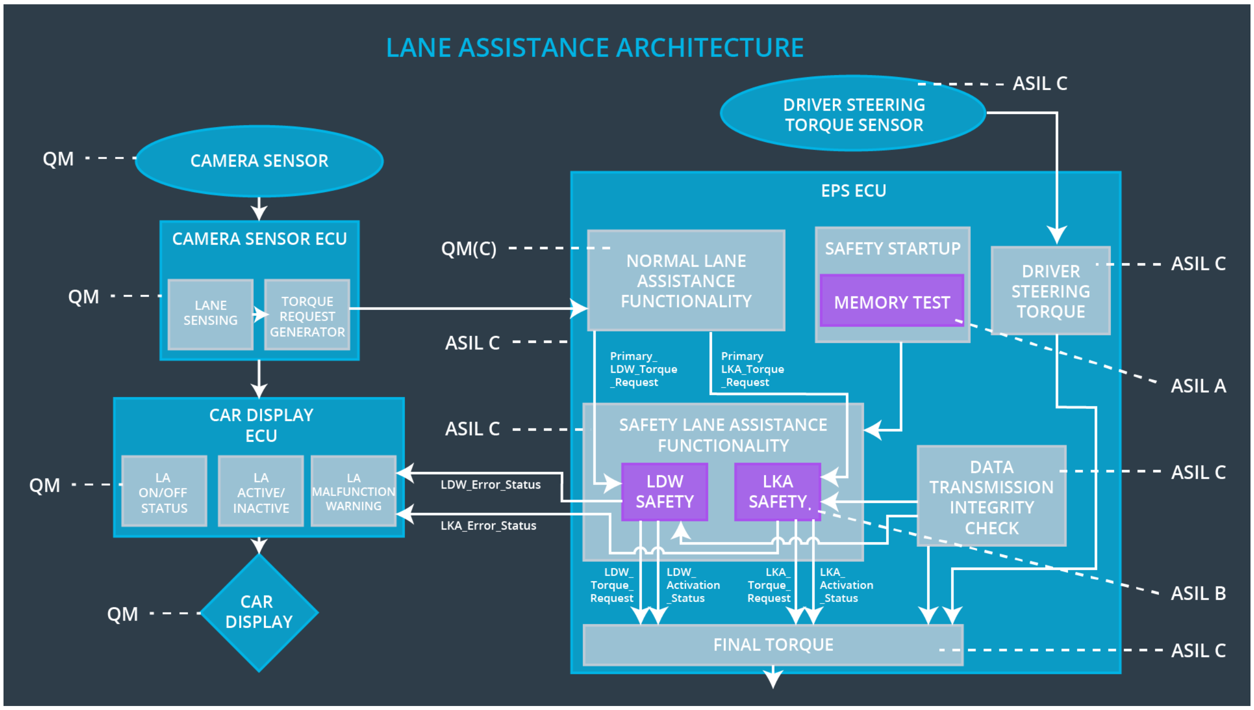
Technical Safety Requirements related to Functional Safety Requirement 01-01 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01-01-01	The LDW safety component shall ensure that the amplitude of the ‘LDW_Torque_Request’ sent to the ‘Final electronic power steering Torque’ component is below ‘Max_Torque_Amplitude’	C	50ms	EPS ECU - LDW Safety Component	Set the oscillating torque to zero.
Technical Safety Requirement 01-01-02	As soon as the LDW function deactivates the LDW feature, the ‘LDW Safety’ software block shall send a signal to the car display ECU to turn on a warning light.	C	50ms	EPS ECU - LDW Safety Component	Set the oscillating torque to zero.
Technical Safety Requirement 01-01-03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the ‘LDW_Torque_Request’ shall be set to zero.	C	50ms	EPS ECU - LDW Safety Component	Set the oscillating torque to zero.
Technical Safety Requirement	The validity and integrity of the data transmission for ‘LDW_Torque_Request’ signal	C	50ms	EPS ECU – Data Transmission	Set the oscillating torque to

01-01-04	shall be ensured.			Integrity Check	zero.
Technical Safety Requirement 01-01-05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition cycle	EPS ECU – Safety Startup	Set the oscillating torque to zero.

2.2. Refined Architecture Diagram from the Technical Safety Concept

The following images shows the refined system architecture:



Technical overview of architecture elements:

Element	Description
Camera Sensor	Sensor for the optical detection of the front area of the vehicle, including detectable lane lines.
Camera Sensor ECU	Electronic Control Unit responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake. Responsible for triggering reactions to add extra torque for LDW and LKA functionality.
Camera Sensor ECU Lane Sensing	Component within the camera sensor ECU responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake.

Camera Sensor ECU Torque Request Generator	Component within the camera sensor ECU responsible for calculating and sending an request for additional steering torque for the LDW and LKA functionality.
Car Display	Visual display which is, among other functionalities, responsible for displaying warning of lane departures and LKA and LDW activation-status.
Car Display ECU	Electronic control unit, which is responsible for creating and providing the data and information that the car display visualizes.
Car Display ECU LA on/off status	Component within the car display ECU responsible for visualizing if the lane assistance functionality is switched on or off.
Car Display ECU LA active/inactive	Component within the car display ECU responsible for visualizing if the lane assistance functionality is active at the moment. Active means the car is drifting away from the center of the lane and LKA is actively acting or the car is getting too narrow to a lane boundary and LDW is warning.
Car Display ECU LA malfunction warning	Component within the car display ECU responsible for visualizing if there occurs any malfunction within the lane assistance system.
Driver Steering Torque Sensor	Sensor responsible for measuring the steering torque provided by the driver.
Electronic Power Steering (EPS) ECU	The electronic control unit is responsible for evaluating the torque provided by the driver and for adding an additional torque based on the torque request of the lane assist system (LKA). Initializes the vibration of the steering wheel when the driver inadvertently drifts away from the center of the lane (LDW).
EPS ECU Normal Lane Assistance Functionality	Component within the electronic power steering ECU responsible for receiving extra torque request from the camera sensor ECU and doing different non-safety tasks.
EPS ECU Driver Steering Torque	Component within the electronic power steering ECU responsible for receiving the steering torque with which the driver moves the steering wheel.
EPS ECU LDW Safety Functionality	Component within the electronic power steering ECU responsible for keeping the lane departure warning action (oscillating torque) below Max_Torque_Amplitude and Max_Torque_Frequency. This component is also responsible for ensuring that the lane departure warning by means of vibration of the steering wheel is only applicated when LDW_On is set.

EPS ECU LKA Safety Functionality	Component within the electronic power steering ECU responsible for ensuring that the lane keeping assistance is not forcing the car longer than Max_Duration to the center of the lane. This component is also responsible for ensuring that the lane keeping assistance by forcing the car to the center of the lane is only applicated when the lane boundaries can be detected reliably.
EPS ECU Final Torque	Component within the electronic power steering ECU responsible for ensuring that the single torque values from LDW, LKA are combined with the drivers original steering torque and sent to the motor.
EPS ECU Safety Startup Memory Test	Component within the electronic power steering ECU responsible for the memory test conducted at startup of the EPS ECU to check for any faults in memory.
EPS ECU Data Transmission Integrity Check	Component within the electronic power steering ECU responsible for checking the data validity and integrity of the data transmission.
Motor	Mechatronic device which adds extra steering torque directly to the steering wheel.

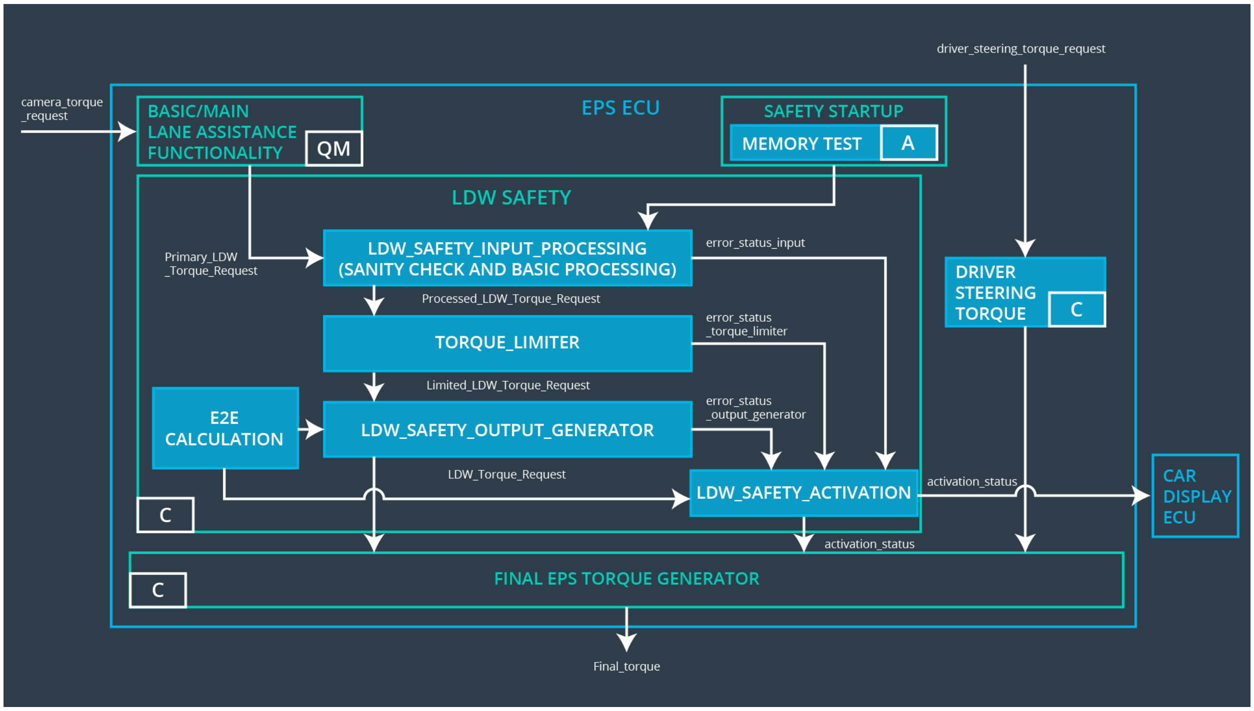
3. Software Requirements

Lane Departure Warning (LDW) Amplitude Malfunction Software Requirements:

Technical Safety Requirement 01-01-01 with its associated parameters
(derived in the technical safety concept):

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01-01	The LDW safety component shall ensure that the amplitude of the ‘LDW_Torque_Request’ sent to the ‘Final electronic power steering Torque’ component is below ‘Max_Torque_Amplitude’	C	50ms	EPS ECU - LDW Safety Component	Set the oscillating torque to zero.

The following image shows the LDW safety component of the EPS ECU:


driver_steering_torque_request
camera_torque_request
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
EPS ECU
SAFETY STARTUP
MEMORY TEST
A
LDW SAFETY
Primary_LDW_Torque_Request
LDW_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
DRIVER STEERING TORQUE
C
Processed_LDW_Torque_Request
error_status_torque_limiter
TORQUE_LIMITER
Limited_LDW_Torque_Request
E2E CALCULATION
LDW_SAFETY_OUTPUT_GENERATOR
error_status_output_generator
LDW_Torque_Request
LDW_SAFETY_ACTIVATION
activation_status
CAR DISPLAY ECU
C
activation_status
C
FINAL EPS TORQUE GENERATOR
Final_torque

Software Safety Requirements related to Technical Safety Requirement 01-01-01 are:

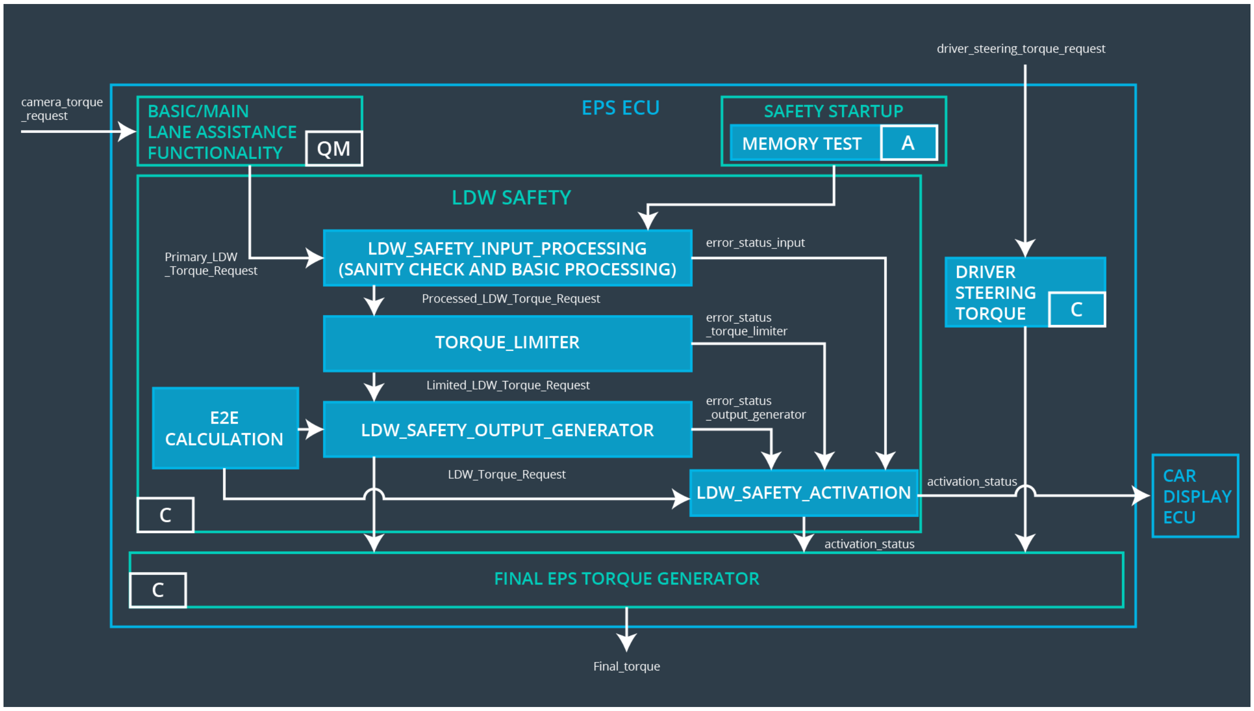
ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-01-01	The input signal “Primary_LDW_Torq_Req” shall be read and pre-processed to determine the torque request coming from the “Basic/Main LAFunctionality” SW Component. Signal “processed_LDW_Torq_Req” shall be generated at the end of the processing.	C	LDW_SAFETY_INPUT_PROCESSING	N/A
Software Safety Requirement 01-01-01-02	In case the “processed_LDW_Torq_Req” signal has a value greater than“Max_Torque_Ampltide_LDW”(maximum allowed safe torque), the torque signal “limited_LDW_Torq_Req” shall be set to 0, else“limited_LDW_Torq_Req” shall take the value of	C	TORQUE_LIMITER	“limited_LDW_Torq_Req” = 0 Nm

	“processed_LDW_Torq_Req”.			
Software Safety Requirement 01-01-01-03	The “limited_LDW_Torq_Req”shall be transformed into a signal “LDW_Torq_Req” whichis suitable to be transmittedoutside of the LDW Safetycomponent (“LDW Safety”) to the “Final EPS Torque”component.	C	LDW_SAFETY_OUTPUT_GENERATOR	LDW_Torq_Req = 0 (Nm)

Technical Safety Requirement 01-01-02 with its associated parameters (derived in the technical safety concept):

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01-02	As soon as the LDW function deactivates the LDW feature, the 'LDW Safety' software block shall send a signal to the car display ECU to turn on a warning light.	C	50ms	EPS ECU - LDW Safety Component	Set the oscillating torque to zero.

The following image shows the LDW safety component of the EPS ECU:


driver_steering_torque_request
camera_torque _request
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
EPS ECU
SAFETY STARTUP
MEMORY TEST
A
LDW SAFETY
Primary_LDW _Torque_Request
LDW_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
DRIVER STEERING TORQUE
C
Processed_LDW_Torque_Request
TORQUE_LIMITER
error_status _torque_limiter
Limited_LDW_Torque_Request
E2E CALCULATION
LDW_SAFETY_OUTPUT_GENERATOR
error_status _output_generator
LDW_Torque_Request
LDW_SAFETY_ACTIVATION
activation_status
CAR DISPLAY ECU
C
activation_status
C
FINAL EPS TORQUE GENERATOR
Final_torque

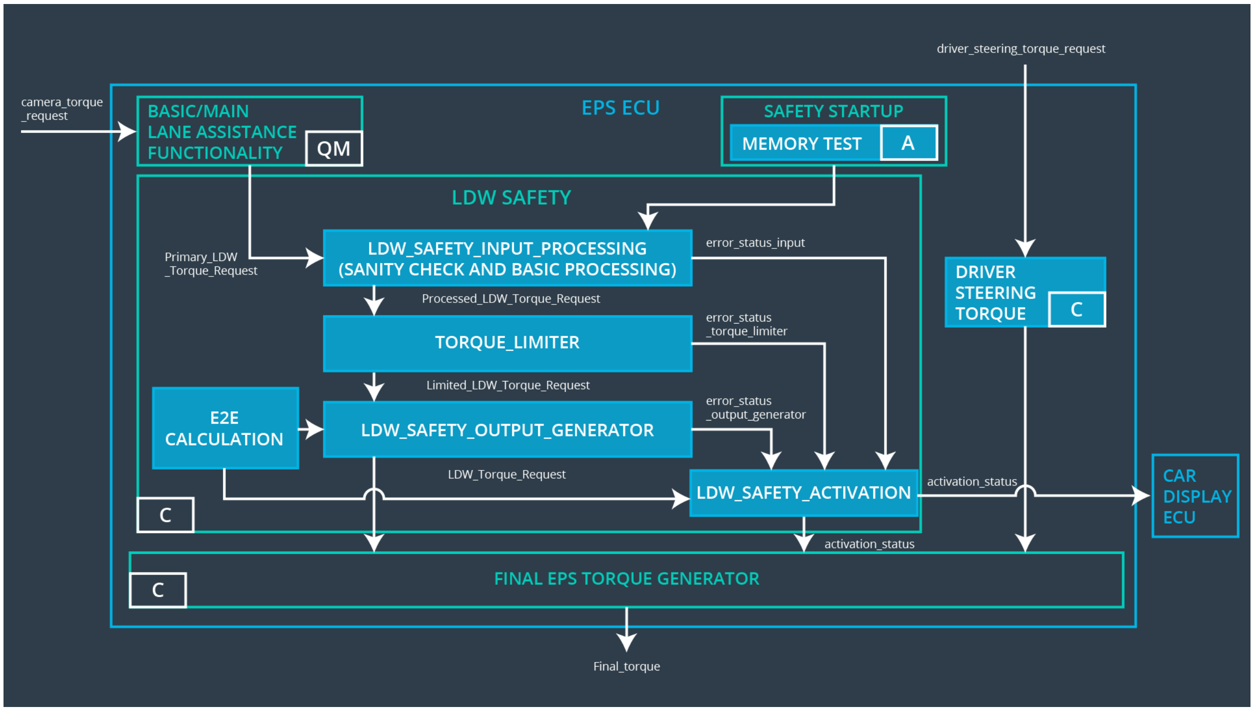
Software Safety Requirements related to Technical Safety Requirement 01-01-02 are:

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-02-01	When the LDW function is deactivated (activation_status set to 0), the activation_status shall be sent to the car display ECU.	C	LDW_SAFETY_ACTIVATION, Car Display ECU	N/A

Technical Safety Requirement 01-01-03 with its associated parameters
(derived in the technical safety concept):

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01-03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the ‘LDW_Torque_Request’ shall be set to zero.	C	50ms	EPS ECU - LDW Safety Component	Set the oscillating torque to zero.

The following image shows the LDW safety component of the EPS ECU:


driver_steering_torque_request
camera_torque_request
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
EPS ECU
SAFETY STARTUP
MEMORY TEST
A
LDW SAFETY
Primary_LDW_Torque_Request
LDW_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
DRIVER STEERING TORQUE
C
Processed_LDW_Torque_Request
TORQUE_LIMITER
error_status_torque_limiter
Limited_LDW_Torque_Request
E2E CALCULATION
LDW_SAFETY_OUTPUT_GENERATOR
error_status_output_generator
LDW_Torque_Request
LDW_SAFETY_ACTIVATION
activation_status
CAR DISPLAY ECU
C
activation_status
FINAL EPS TORQUE GENERATOR
C
Final_torque

Software Safety Requirements related to Technical Safety Requirement 01-01-03 are:

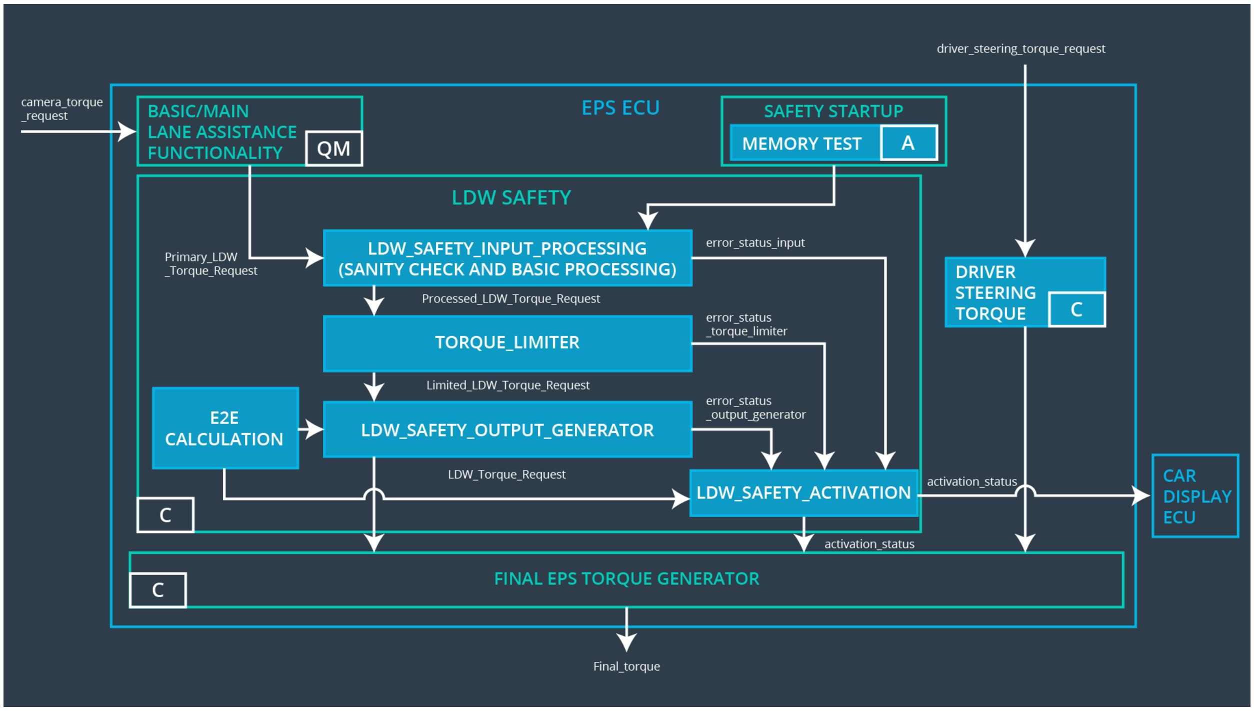
ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-03-01	Each of the SW elements shall output a signal to indicate any error which is detected by the element.	C	All	N/A

	Error signals: error_status_input (LDW_SAFETY_INPUT_PROCESSING) error_status_torque_limiter (TORQUE_LIMITER) error_status_output_gen (LDW_SAFETY_OUTPUT_GENERATOR)			
Software Safety Requirement 01-01-03-02	A software element shall evaluate the error status of all the other software elements and in case any one of them indicates an error, it shall deactivate the LDW feature. (“activation_status”=0)	C	LDW_SAFETY_ACTIVATION	Activation_status = 0 (LDW function deactivated)
Software Safety Requirement 01-01-03-03	In case of no errors from the software elements, the status of the LDW feature shall be set to activated. (“activation_status”=1)	C	LDW_SAFETY_ACTIVATION	N/A
Software Safety Requirement 01-01-03-04	In case an error is detected by any of the software elements, it shall set the value of its corresponding torque to 0 so that “LDW_Torq_Req” is set to 0.	C	All	LDW_Torq_Req = 0
Software Safety Requirement 01-01-03-05	Once the LDW functionality has been deactivated, it shall stay deactivated till the time the ignition is switched from off to on again.	C	LDW_SAFETY_ACTIVATION	Activation_status = 0 (LDW function deactivated)

Technical Safety Requirement 01-01-04 with its associated parameters (derived in the technical safety concept):

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01-04	The validity and integrity of the data transmission for ‘LDW_Torque_Request’ signal shall be ensured.	C	50ms	EPS ECU – Data Transmission Integrity Check	Set the oscillating torque to zero.

The following image shows the LDW safety component of the EPS ECU:


driver_steering_torque_request
camera_torque_request
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
EPS ECU
SAFETY STARTUP
MEMORY TEST
A
LDW SAFETY
Primary_LDW_Torque_Request
LDW_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
Processed_LDW_Torque_Request
TORQUE_LIMITER
error_status_torque_limiter
Limited_LDW_Torque_Request
E2E CALCULATION
LDW_SAFETY_OUTPUT_GENERATOR
error_status_output_generator
LDW_Torque_Request
LDW_SAFETY_ACTIVATION
activation_status
C
DRIVER STEERING TORQUE
C
CAR DISPLAY ECU
activation_status
FINAL EPS TORQUE GENERATOR
C
Final_torque

Software Safety Requirements related to Technical Safety Requirement 01-01-04 are:

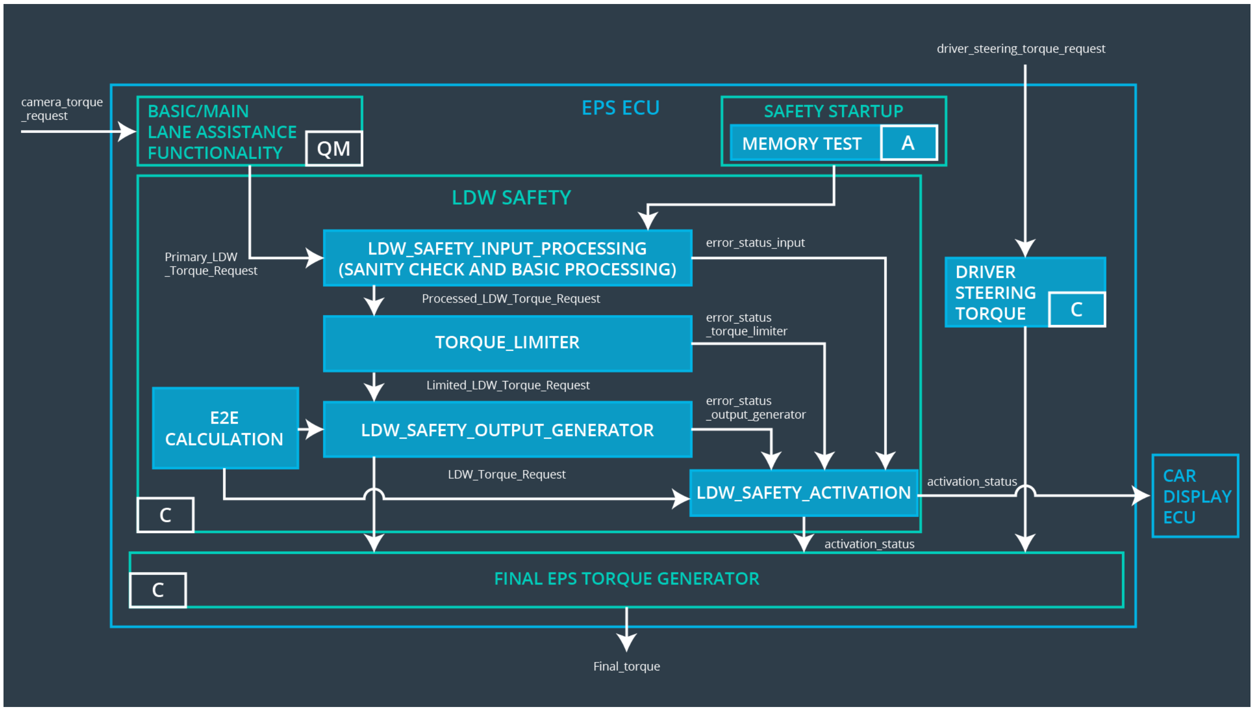
ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-04-01	Any data to be transmitted outside of the LDW Safety component (“LDW Safety”) including "LDW_Torque_Req" and “activation_status” shall be protected by an End2End (E2E) protection mechanism.	C	E2ECalc	LDW_Torq_Req = 0 (Nm)

Software Safety Requirement 01-01-04-02	The E2E protection protocol shall contain and attach the control data: alive counter (SQC) and CRC to the data to be transmitted.	C	E2ECalc	LDW_Torq_Req = 0 (Nm)

Technical Safety Requirement 01-01-05 with its associated parameters (derived in the technical safety concept):

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01-05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition cycle	EPS ECU – Safety Startup	Set the oscillating torque to zero.

The following image shows the LDW safety component of the EPS ECU:


driver_steering_torque_request
camera_torque_request
EPS ECU
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
SAFETY STARTUP
MEMORY TEST
A
LDW SAFETY
Primary_LDW_Torque_Request
LDW_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
Processed_LDW_Torque_Request
TORQUE_LIMITER
error_status_torque_limiter
Limited_LDW_Torque_Request
E2E CALCULATION
LDW_SAFETY_OUTPUT_GENERATOR
error_status_output_generator
LDW_Torque_Request
LDW_SAFETY_ACTIVATION
activation_status
activation_status
C
DRIVER STEERING TORQUE
C
CAR DISPLAY ECU
FINAL EPS TORQUE GENERATOR
C
Final_torque

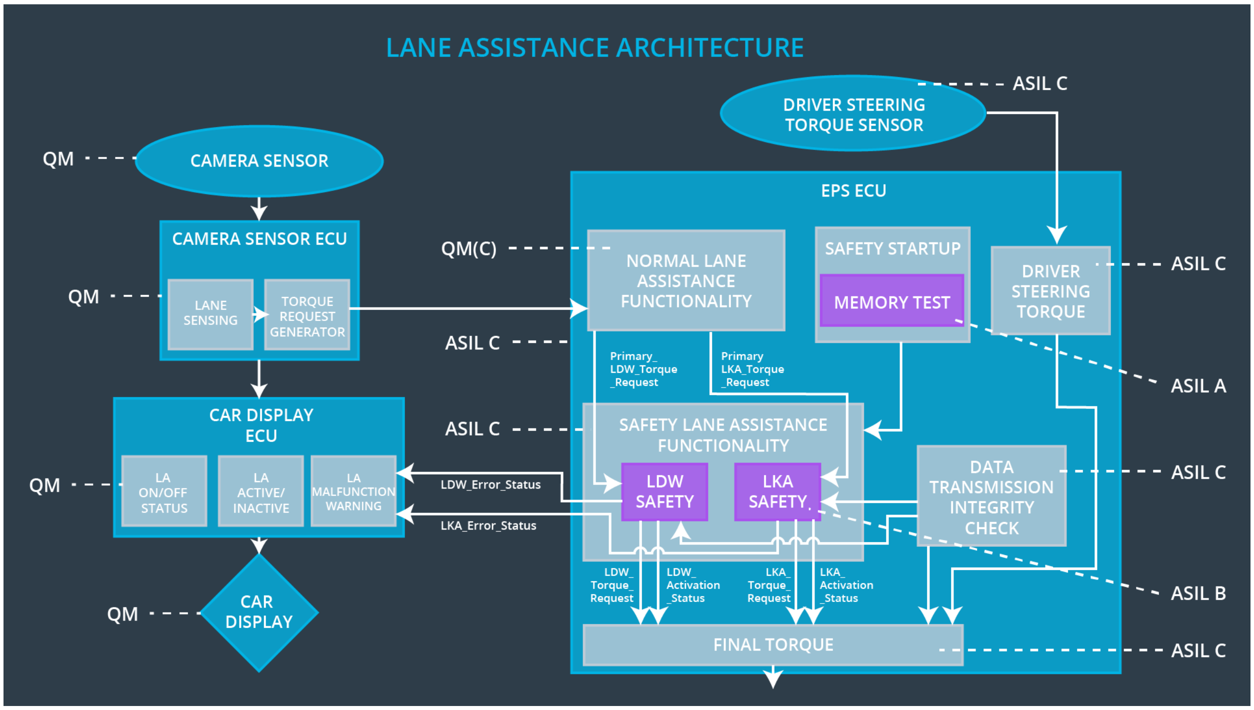
Software Safety Requirements related to Technical Safety Requirement 01-01-05 are:

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-05-01	A CRC verification check over the software code in the Flash memory shall be done every time the ignition is switched from off to on to check for any corruption of content.	A	MEMORY TEST	Activation_status = 0

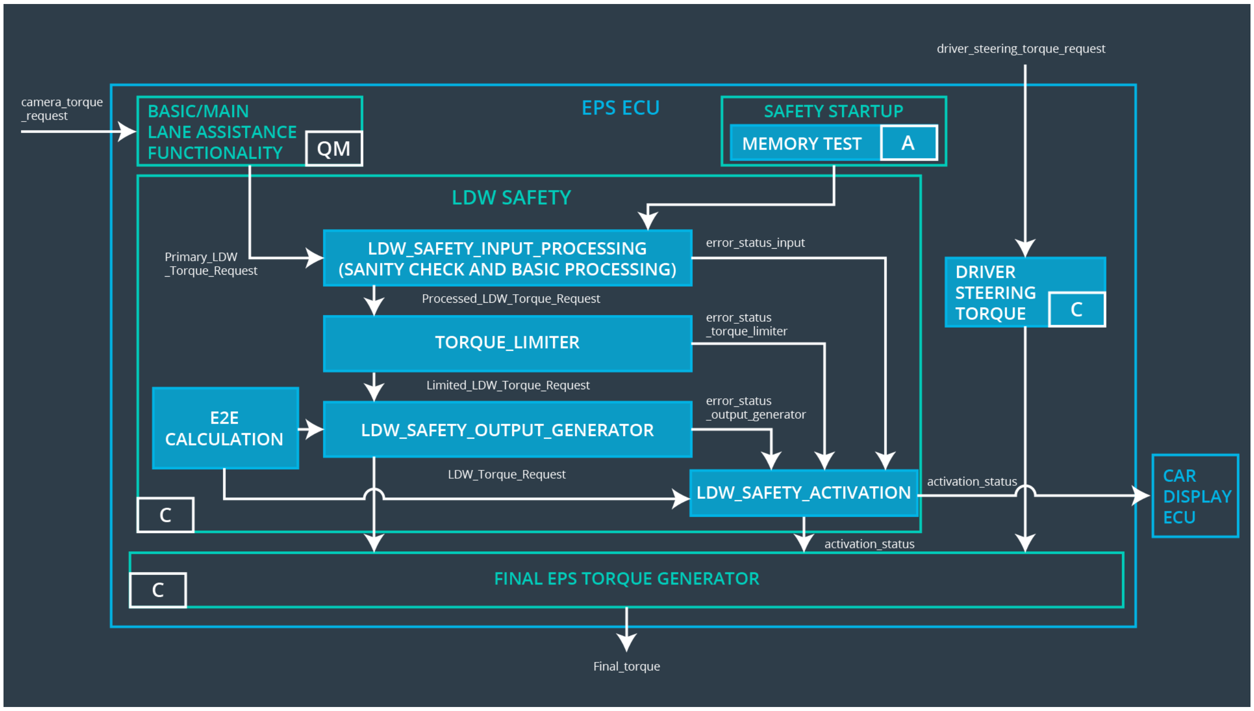
Software Safety Requirement 01-01-05-02	Standard RAM tests to check the data bus, address bus and device integrity shall be done every time the ignition is switched from off to on (E.g.: walking 1s test, RAM pattern test. Refer RAM and processor vendor recommendations).	A	MEMORY TEST	Activation_status = 0
Software Safety Requirement 01-01-05-03	The test result of the RAM or Flash memory shall be indicated to the LDW_Safety component via the "test_status" signal.	A	MEMORY TEST	Activation_status = 0
Software Safety Requirement 01-01-05-04	In case any fault is indicated via the "test_status" signal the INPUT_LDW_PROCESSING shall set an error on error_status_input (=1) so that the LDW functionality is deactivated and the LDW_Torque is set to 0.	A	LDW_SAFETY_INPUT_PROCESSING	Activation_status = 0

4. Refined Architecture Diagram

The following images shows the refined system architecture:



The following image shows the LDW safety component of the EPS ECU:


driver_steering_torque_request
camera_torque _request
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
EPS ECU
SAFETY STARTUP
MEMORY TEST
A
LDW SAFETY
Primary_LDW _Torque_Request
LDW_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
DRIVER STEERING TORQUE
C
Processed_LDW_Torque_Request
TORQUE_LIMITER
error_status _torque_limiter
Limited_LDW_Torque_Request
E2E CALCULATION
LDW_SAFETY_OUTPUT_GENERATOR
error_status _output_generator
LDW_Torque_Request
LDW_SAFETY_ACTIVATION
activation_status
CAR DISPLAY ECU
C
activation_status
C
FINAL EPS TORQUE GENERATOR
Final_torque